



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,533	07/14/2001	Myles Jordan	063170.6294	3486
5073	7590	09/27/2007	EXAMINER	
BAKER BOTTS L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980			PYZOCHA, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2137	
			NOTIFICATION DATE	DELIVERY MODE
			09/27/2007	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com  
glenda.orrantia@bakerbotts.com

# Office Action Summary

Application No.

09/905,533

Applicant(s)

JORDAN, MYLES

Examiner

Michael Pyzocha

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 07 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 9/7/07.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims 1-18 are pending.
2. A request for continued examination under 37 CFR 1.114 was filed in this application after appeal to the Board of Patent Appeals and Interferences, but prior to a decision on the appeal. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 09/07/2007 has been entered.

### ***Information Disclosure Statement***

3. The information disclosure statement (IDS) submitted on 09/07/2007 was filed after the mailing date of the Examiner's Answer on 07/30/2007. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

### **Claim Rejections - 35 USC § 103**

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the

Art Unit: 2137

differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4, 6-14, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, U.S. Patent No. 6,357,008, in view of Trcka, U.S. Patent No. 6,453,345.

As per claims 1-2, 7-12, and 17-18, the applicant describes a method for detecting decryption of encrypted viral code comprising the following limitations which are met by Nachenberg and Trcka:

- a) emulating computer executable code in a subject file (Nachenberg: Col 7, lines 9-12);
- b) maintaining a list of memory regions that have been read and then modified during emulation (Nachenberg: Col 9, lines 5-10);
- c) flagging a memory area that is read during emulation of a first instruction in the computer executable code (Nachenberg: Col 9, lines 5-10);
- d) detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code (Nachenberg: Col 9, lines 5-10);
- e) updating the list of memory regions to include the modified flagged memory area (Nachenberg: Col 9, lines 11-14);

Art Unit: 2137

f) determining that one of the listed memory regions is larger than a predetermined size (Nachenberg: Col 8, lines 1-30);

g) triggering a viral detection in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code (Nachenberg: Col 8, lines 1-30; Trcka: Col 17, lines 24-34);

Nachenberg discloses all the limitations of the above claim except for part f. With regard to part f, Nachenberg discloses that if a memory region is not larger than a predetermined size it is regarded as non-viral and a first particular course of action is followed (e.g. directly entering the exploration phase). If a memory region is larger than a predetermined size, a second course of action is followed. However, Nachenberg does not disclose a viral detection alarm.

Trcka discloses the idea of a viral detection alarm. The use of an alarm serves many benefits, including alerting a user so that a user is informed and may take appropriate action. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Trcka with those of Nachenberg and use an alarm because doing so

Art Unit: 2137

alerts a user so that he is informed of the situation and may take appropriate action.

As per claims 3 and 13, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is met by Nachenberg: Wherein the emulation is performed on an instruction-by-instruction basis (Nachenberg: Col. 7, lines 55-67).

As per claims 4, 6, 14, and 16, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is met by Nachenberg:

a) determining whether a selected one of the listed memory regions overlaps the modified memory area (Nachenberg: Figure 4B);

b) updating the selected memory region to encompass the modified memory area (Nachenberg: Col. 9, lines 11-14).

6. Claims 5 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, U.S. Patent No. 6,357,008, in view of Trcka in further view of Nachenberg, U.S. Patent No. 6,971,019.

As per claims 5 and 15, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of

Art Unit: 2137

Trcka, with the following limitation which is anticipated by Nachenberg:

a) determining whether a selected one of the listed memory regions is contiguous with the modified memory area (Nachenberg: Figure 4B);

b) updating the selected memory region to encompass the modified memory area (Nachenberg: Col 9, lines 11-14).

Regarding part a, Nachenberg (#6,357,008) in view of Trcka discloses comparing a selected one of the listed memory regions with the modified memory area but does not specifically disclose a determination that the regions are contiguous. Nachenberg (#6,971,019) discloses the well-known idea of determining a continuous memory area. It would have been obvious to one of ordinary skill in the art to combine the ideas of Nachenberg (#6,971,019) with those of Nachenberg (#6,357,008) in view of Trcka because doing so provides a further means to monitor for viral code.

### **Conclusion**

7. All claims are drawn to the same invention claimed in the application prior to the entry of the submission under 37 CFR 1.114 and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered

Art Unit: 2137

in the application prior to entry under 37 CFR 1.114.

Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action after the filing of a request for continued examination and the submission under 37 CFR 1.114. See MPEP § 706.07(b).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.



Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

PTO-1449		Application No. 09/905,533		Applicant(s) Myles Jordan	
<b>Information Disclosure Citation In an Application</b>		Docket Number 063170.6294	Group Art Unit 2137	Filing Date July 14, 2001	

U.S. PATENT DOCUMENTS							
		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE
A		2002/0073330 A1	06/13/2002	Chandnani et al.	713	200	07/14/2001
B		2002/0083334 A1	06/27/2002	Rogers et al.	713	200	07/14/2001
C		2002/0091934 A1	07/11/2002	Jordan	713	188	07/14/2001
D		7,069,583 B2	06/27/2006	Yann et al.	726	4	07/14/2001
E		7,069,589 B2	06/27/2006	Schmall et al.	726	24	07/14/2001
F		7,210,040 B2	04/24/2007	Jordan	713	187	07/14/2001

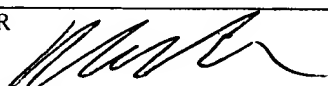
  

FOREIGN PATENT DOCUMENTS								
		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
G								
H								
I								
J								
K								

		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
L			
M			
N			
O			
P			
Q			
R			

EXAMINER 	DATE CONSIDERED 9/17/07
---	----------------------------

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

U.S. PATENT AND TRADEMARK OFFICE